

EXHIBIT 1



Brad A. Lebow
(858) 550-6084
blebow@cooley.com

VIA MAIL AND E-MAIL

August 21, 2012

John Lowther
Kate DiDonato
DOYLE LOWTHER LLP
10200 Willow Creek Road, Suite 150
San Diego, CA 92131

Helen I Zeldes
Aaron Olsen
Amber Eck
ZELDES & HAEGGQUIST, LLP
625 Broadway, Suite 906
San Diego, CA 92101

RE: *In re Sony VAIO Computer Notebook Trackpad Litigation*
U.S. District Court for the Southern District of California
Case No. 09-CV-2109 AJB (MDD)

Dear Counsel:

We write to confer regarding: (1) scheduling the examination of plaintiff Egner's Sony VAIO NW240F/P notebook computer (see Sony's Request for Production No. 79 and plaintiff's Response to Sony's Request for Production No. 79); and (2) scheduling plaintiff's deposition.

First, as we have previously discussed, we intend to conduct a hardware and software forensics examination of plaintiff's notebook computer. We will need two days to complete examination. We request that the examination occur during the week of September 24, 2012. But please note that we are available for the hardware examination on September 24, 27, or 28 only, while we are available for the entire week for the software forensic examination. For the examination, we are attaching the proposed hardware and software forensic protocols. Please confirm that these protocols are acceptable to plaintiff.¹

Second, we intend to take plaintiff's deposition in San Diego, CA. We request that plaintiff's deposition occur during either the week of October 8 (but not October 12) or October 15, 2012. Please let us know when plaintiff is available during those two weeks.

Sincerely,



Brad A. Lebow

cc: Michelle Doolin
Leo P. Norton
Michael A. Geibelson
Elizabeth D. Le

¹ The protocols are also subject to approval from Best Buy Stores, L.P.



PROTOCOL FOR OBSERVATION AND INVESTIGATION OF TOUCHPAD

Necessary equipment: ESD wrist strap, ESD smock, magnifying glass, stereoscope, multimeter, digital camera, #0 and #1 Philips Screwdriver, Small (4mm) Flat-head Screwdriver, Non-marking Scribe or Pick, Thumb Forceps or Tweezers, Orange Stick or Bamboo Spatula, containers for the various screws, cotton gloves.

Initial visual inspection and evaluation

1. Visual inspection of the laptop. Photo-document Unit ID Label on bottom of unit. Photo-document any anomalies, including evidence of damage or mishandling.
2. Open laptop. Photo-document Model ID Label on lower right-hand corner of LCD Bezel. Photo-document Touchpad. Photo-document any anomalies, including evidence of damage or mishandling.
3. Retrieve AC Power Cord. Photo-document all identifiers and any anomalies. Plug AC Power Cord into the Power Jack. Plug AC Power Cord into AC outlet. Turn on laptop by depressing the Power button.
4. Once access to a Windows screen is obtained, assess operation of Touchpad. Document any anomalous behavior, such as track in reverse, freeze or fail to register input, or randomly open or close windows.
5. Unplug AC Power Cord. Re-assess operation of Touchpad in a similar manner as described above.
6. Turn off the laptop through the Shutdown option in Windows.

Disassembly: All anomalies noted during disassembly will be photo-documented

7. Turn over the laptop so the top side is in contact with the table.
8. Remove the Battery Pack by sliding the lock and release levers.
9. Remove the Hard Drive removing two screws from the Hard Drive Door. Slide the Hard Drive Door downward to release the three tabs and rotate towards the Top. Remove two additional screws from the Hard Drive. Slide the Hard Drive to the Left by the Mylar tab and then lift out of the unit.
10. Remove the Optical Drive by removing two screws and sliding the Optical Drive to the left.



11. Remove Keyboard by removing three screws. Open the laptop slightly, while still in the down position, and release three tabs underneath the Optical Drive by inserting a non-marking object in the circular indentation shown and pressing downward. Turn over the laptop so the bottom side is in contact with the table and rotate the Keyboard towards the Touchpad and release the Keyboard Connector. Adhesive tape may need to be removed.
12. Photo-document condition of Touchpad Cable.
13. Turn over the laptop so the top side is in contact with the table.
14. Remove the Bottom Housing by removing sixteen (16) different screws and rotating the bottom housing from the top.
15. Remove the Cooling Unit by disconnecting the Fan Cable and two connectors on the Display Harness from the Motherboard by lifting straight up. Remove the tape and note the Routing Guides for assembly.
 - a. If Internal Graphics, remove two screws from the Fan. Remove four screws (of a different type) from the Cooling Unit over the CPU. Lift the Cooling Unit up. Note - the NB Sink for the GPU is a separate part. For Motherboard Removal, the NB Sink must be removed first. Remove three screws and lift the NB Sink up.
 - b. If External Graphics, remove two screws from the Fan. Remove seven screws (of a different type) - four over the CPU and three over the GPU. Remove the Tape securing the RJ45 Cable to the Cooling Unit. Lift the Cooling Unit straight up to remove. During assembly, ensure the RJ45 Cable is routed as shown and the tape reapplied over the Cooling Unit.
16. Turn over the laptop so the bottom side is in contact with the table and disconnect the Touchpad Cable and Power Button Board Cable from underneath the Keyboard.
17. Turn over the laptop so the top side is in contact with the table and disconnect the DC In Cable, Camera Cable, Speaker Cable, RJ45 Cable, and USB Board Cable from the Motherboard.
18. Remove three screws from the Motherboard and gently raise the left side of the Motherboard to release the side I/O ports and remove to the Left.
19. Visually inspect and photo-document the componentry on the Motherboard that controls the Touchpad.



Touchpad Removal and Inspection: Any and all anomalies noted during Touchpad removal and inspection will be photo-documented

20. Visually inspect and photo-document the area of the Touchpad circuit card observable after removal of the Motherboard. Place the Touchpad circuit card under stereoscope for closer inspection.
21. Curve trace each pin of the microcontroller on the Touchpad circuit card.
22. Release the Lock Lever by rotating downward and remove the Touchpad Cable from the Touchpad.
23. Using a non-marking tool, loosen the adhesive with gentle pressure below the Touchpad Buttons.
24. Using a non-marking tool, loosen the adhesive with gentle pressure beginning the thinnest area below the Touchpad Buttons. Loosen the adhesive on each side and then the top of the Touchpad.
25. Gently lift the Touchpad Block from top to remove.
26. Visually inspect and photo-document the bottom side of the Touchpad circuit card. Place the Touchpad circuit card under stereoscope for closer inspection.
27. Curve trace or resistance measure other components on the Touchpad circuit card as appropriate.
28. Remove the Touchpad circuit card from the frame.
29. Visually inspect and photo-document the top side of the Touchpad circuit card. Place the Touchpad circuit card under stereoscope for closer inspection.
30. Curve trace or resistance measure other components on the Touchpad circuit card as appropriate.

Sony representative with experience will re-assemble the laptop.



PROTOCOL FOR FORENSIC IMAGING

The computer/device forensic imaging protocol will be followed for the imaging process and, if applicable, any future computer/device forensic imaging. The following procedures are based upon computer forensic industry standards.

1. The forensic collection specialist will procure and sanitize a new hard drive(s), which will be used for creating two bit-by-bit certified images of the original hard drive(s), one image to be kept pristine and one image to be used as a working copy.
2. The hard drive will be physically removed from the laptop(s) to be imaged and attached to one side of an industry recognized forensic imaging hardware device. The laptop hardware will be physically inspected and any modifications or abnormalities will be documented (e.g. extra RAM added, or visible liquid damage). Upon removal of the hard drive from the computer(s), the computer will be powered on to obtain and document the BIOS date and time.
3. The sanitized hard drive(s) will be attached to the opposite side of the same forensic imaging hardware device(s).
4. The forensic imaging device(s) used must incorporate an industry approved write blocker which is used to protect the original hard drive's data by placing the drive in "read-only" mode, prohibiting any changes to the data stored on the original hard drive.
5. Once the forensic imaging process is complete, the image will be verified by using an MD5 hash value (aka a digital fingerprint).
6. Both the original hard drive(s) and the imaged hard drive(s) will be disconnected from the forensic imaging device.
7. The original hard drive(s) will be reinserted back in to the original computer(s).
8. If iDiscovery Solutions deems that it is better to leave the original hard drive in the laptop for imaging, then an industry standard forensic software program capable of being run from CD will instead be used for creating the forensic images. Further, if the laptop is using encryption, the Plaintiff will provide the login credentials so iDiscovery Solutions can instead perform a live forensic image.
9. The computer/laptop(s) will be returned to the custody and control of the individual or "owner" as directed by legal counsel.
10. The forensic images will remain in the possession of iDiscovery Solutions for analysis purposes, and iDiscovery Solutions will recover all partitions and all folders prior to the start of any forensic analysis.
11. Once the case is "closed" iDiscovery Solutions will forensically wipe the data from the imaged hard drive(s), and if requested, provide an Affidavit of such actions.



Forensic Scope

The forensic investigation of each computer's hard drive(s) is specifically limited to the areas identified and listed below:

1. Documentation of each Computer's Make, Model, and Serial Number:
 - a. List the Make of the computer;
 - b. List the Model of the computer;
 - c. List the Serial Number of the computer;
 - d. Include a minimum of three pictures of the computer:
 - i. One picture showing the front of the computer (from the user's perspective); and
 - ii. One picture of the bottom of the computer; and
 - iii. One picture of the "tag" with the Make, Model and Serial Number of the computer, if available.
2. Documentation of the Hard Drive(s) located inside each computer:
 - a. Two pictures of each hard drive(s) mounted inside each computer:
 - i. One picture showing the "top" side of the hard drive where the manufacturer's label is located; and
 - ii. One picture showing the underside area of the hard drive.
3. Documentation of Registry Files (including current, restore points, and/or deleted files related to the Registry):
 - a. List all Windows accounts, including all administrator accounts, system accounts and user accounts, and include documentation of the following information for each account:
 - i. When the account was created;
 - ii. When the account was last accessed (used).
 - b. Investigate and document the existence of any type of external device (e.g., thumb drives, CD-ROMs, DVDs, external hard drives, etc.), ever associated with any Computer's hard drive(s). If identified, document the device according to the instructions contained in the "Reporting" section.



- c. Investigate and document the Most Recently Used (MRUs). When identified, document the MRUs in their specific order according to the instructions contained in the "Reporting" section.
 - d. Investigate and document the format date of the hard drive(s)
 - e. Investigate and document all dates of installation (and/or reinstallation) of the Windows Operating system, including any and all upgrades or service patches, if available. When identified, document all installation and/or reinstallation dates according to the instructions contained in the "Reporting" section.
 - f. Investigate and document the dates, types of software, manufacturers of any software, and name(s) of any software used to potentially wipe, erase, or shred data on any computer hard drive(s). If identified, document the findings by computer and computer hard drive according to the instructions contained in the "Reporting" section.
 - g. Investigate and document the dates, types of software, manufacturers of any software, versions and name(s) of any software used to perform virus scans.
 - h. Investigate and document the dates, types of software, manufacturers of any software, versions and name(s) of any software or hardware driver associated to a touchpad or other internal or external navigational device such as a mouse, trackball, etc.
4. User Created/Help Files: Microsoft Word, Microsoft Excel, Microsoft Power Point, Microsoft Access, Corel Word Perfect, User Manuals, Readme files, etc., as well as container files such as zip, rar, gzip, 7zip, etc.
- a. Locate, identify and document any and all file(s) which contain a match(es) to the key search terms identified on the document "Key Search Terms" (Allocated Space).
 - b. Locate, identify and document any and all file(s) deleted, yet recoverable, which contain a match(es) to the key search terms identified on the document "Key Search Terms".
 - c. If any of the information requested in either 4(a) or 4(b) is located, follow the process contained in the "Reporting" section.
5. Email (non-privileged): PST, OST, NSF, MSG, web-based email, etc.
- a. Locate, identify and document any active or recoverable email or attachment which contain a match(es) to the key search terms identified in the section "Key Search Terms".
 - b. Locate, identify and document any email deleted, yet recoverable, which contain a match(es) to the key search terms identified in the section "Key Search Terms".



- c. If any of the information requested in either 5(a) or 5(b) is located, follow the process contained in the "Reporting" section.

6. Internet History:

- a. Search, locate, identify and list which Internet browser was (or is) being used and the version of every browser located and identified. When identified, document the Internet browser(s) used on the computer hard drive(s) according to the instructions contained in the "Reporting" section.
- b. Search, locate, identify and list all web sites accessed, including all dates and times related to each web site visit that would tend to identify visits to sites (e.g. list serves, forums) for reviewing information about, or for downloading software or hardware drivers associated to a touchpad or other internal or external navigational device such as a mouse, trackball, etc. When identified, document the web sites, including the dates and times related to each web site according to the instructions contained in the "Reporting" section.
- c. Identify all Internet searches associated to 6b above, such as dates, times and any other available information about searches performed on Google, MSN, Yahoo, etc.

7. Prefetch Folders/Files:

- a. Investigate and document the existence of any prefetch files that tend to show the execution of programs, including all dates, times and other associated metadata.

8. Link Files/Shortcuts:

- a. Investigate and document the existence of any link file(s) that show files being opened from any remote location, CD/DVD or an externally connected device.

9. Info2 File Analysis:

- a. Investigate and document all Info2 records, including all available metadata.

10. Encrypted/Password Protected Files:

- a. Investigate and document all encrypted and/or password protected documents that are unable to be searched without retrieving the password.

11. Unallocated Space:

Search the unallocated space from each computer hard drive, plus 50 characters before or after of readable text using the key search terms found in the section "Key Search Terms". If a "match" or a "hit" is found or identified, extract and document the contents of the "match" or "hit" according to the instructions contained in the "Reporting" section.



Key Search Terms

1. Trackp*
2. Touchp*
3. Track pad
4. Touch pad
5. Pointer
6. Curser
7. Mouse

The search terms below will be further limited as follows: (Sony or VAIO or Trackp*or Touchp* or Track pad or Touch pad or Pointer or Curser or Mouse) w/20 (INSERT EACH SEARCH TERM FROM LIST BELOW)

8. Defect
9. Issue
10. Problem
11. Freez*
12. Fail*
13. Erratic

Reporting

The following information and reporting requirements apply to each Section of the forensic protocol. (NOTE: The forensic investigation of the hard drive(s) is specifically limited to the areas identified and listed within this forensic protocol.)

1. Extract and provide to Defendant's counsel, except privileged emails, a forensically sound copy of each email, attachment and/or document and include the following attributes:
 - a. Complete file name;
 - b. Dates and times related to Created, Modified/Last Written, and Last Access;
 - c. Sent Date and Time;
 - d. Sender;



- e. Recipient(s);
 - f. Subject Line;
 - g. Attachment Name;
 - h. Entire Path of where the file was located:
 - i. If the information is discovered in allocated space, the path shall include the following:
 - 1. Partition Drive letter;
 - 2. All folder structures leading up to the file name;
 - 3. File name; and
 - 4. Any symbolic folder information related to their respective paths.
 - ii. If the information is found in unallocated space, the path/information will contain the sector-by-sector address where the information was discovered.
 - i. The state of the file (e.g., if the file was deleted or not deleted);
 - j. Both physical and logical size of the file;
 - k. HASH value of the file;
 - l. Contents of the file in digitally native format;
 - m. Contents of the file converted to PDF/TIFF format;
 - n. List each author, where available, to each file.
- 2. If the search hit is related to fragmented information, the information will be extracted from the beginning point of where the fragmented information was first discovered, to the ending point of where the information was discovered.
 - 3. Plaintiff's counsel will provide a list of privilege email addresses and domains. iDiscovery Solutions will not review the email contents, but will instead isolate the responsive emails for review by Plaintiff's counsel.
 - 4. Emails deemed privileged by Plaintiff's counsel will be placed onto a privilege log for review by Defendants counsel. The privilege log shall contain the information required by the Federal Rules of Civil Procedure, any applicable Local Civil Rule, or as agreed to by the parties in writing.